PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2000-315177**

(43)Date of publication of application : **14.11.2000**

(51)Int.Cl. G06F 12/14
G06F 17/30
H04N 5/91

(21)Application number : **11-124182**

(22)Date of filing : **30.04.1999**

(71)Applicant : **TOSHIBA CORP**

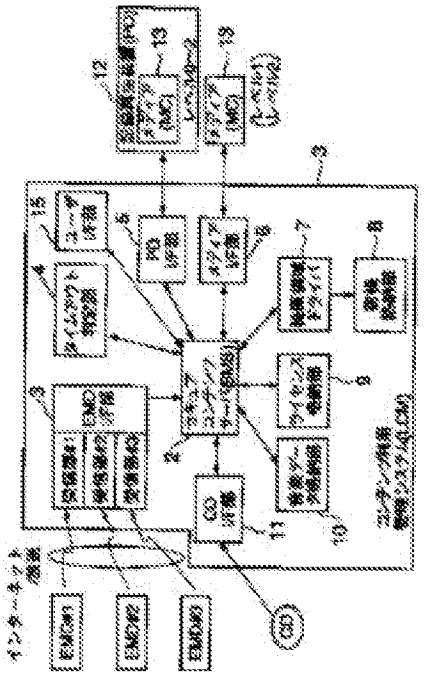
(72)Inventor : **TAMURA MASABUMI**
KAMIBAYASHI TATSU
YAMADA HISASHI
ISHIBASHI YASUHIRO
KATO HIROSHI
TOMA HIDEYUKI

(54) METHOD AND DEVICE FOR CONTENTS MANAGEMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To obtain the contents managing method which limits the duplication of contents and protects the copyright of the contents by checking out from the number of contents which can be copied each time duplicate contents are recorded on a storage medium when an indication for duplicate recording to the storage medium is received.

SOLUTION: An LCM 1 is equipped with a secure contents server(SMS) 2 and contents are stored on an SMS 2. The SMS 2 outputs contents data to media (MC) 13. The SMS 2 subtracts '1' from the rest number of contents of checkout requests of a hotel book and erases information stored in areas corresponding to the folders of the contents on the MC 13 by overwriting random numbers. Then the SMS 2 receives the values of the respective areas after overwriting transferred from the MC 13 so as to confirm the overwriting erasure and checks them. Consequently, the number of duplicate contents is efficiently restricted to protect the copyright of the contents.



(19)日本国特許庁（Ｊ Ｐ）　(12) **公 開 特 許 公 報（Ａ）**　(11)特許出願公開番号
特開2000－315177
（P2000－315177A）
(43)公開日　平成12年11月14日(2000.11.14)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ		テーマコード*（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	５Ｂ０１７
			３２０Ｂ	５Ｂ０７５
17/30		15/40	３２０Ｚ	５Ｃ０５３
Ｈ０４Ｎ　5/91			３７０Ｇ	
		Ｈ０４Ｎ　5/91	Ｐ	

審査請求　未請求　請求項の数14　ＯＬ　（全 20 頁）

(21)出願番号　特願平11－124182

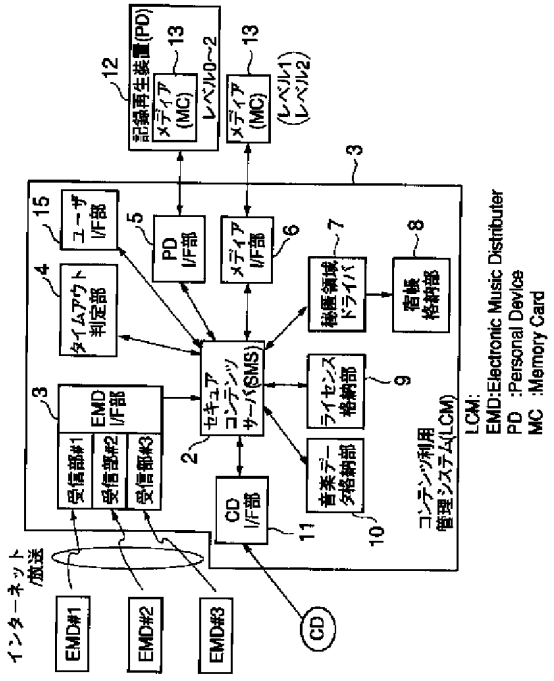
(22)出願日　平成11年４月30日(1999.4.30)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　田村　正文
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内
(72)発明者　上林　達
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　コンテンツ管理方法およびコンテンツ管理装置

(57)【要約】
【課題】記憶媒体に記録できる複製コンテンツの数を規制することによりコンテンツの複製を制限して、コンテンツの著作権を保護することのできるコンテンツ管理方法を提供する。
【解決手段】記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法であって、前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを１つ記録する毎に前記複製可能コンテンツ数から１減算し、また、該記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該複製コンテンツを１つ消去する毎に前記複製可能コンテンツ数を１加算することを特徴とするコンテンツ管理方法。



【特許請求の範囲】
【請求項１】　記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法であって、
前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを１つ記録する毎に前記複製可能コンテンツ数から１減算し、また、該記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該複製コンテンツを１つ消去する毎に前記複製可能コンテンツ数を１加算することを特徴とするコンテンツ管理方法。
【請求項２】　前記記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報を記録することを特徴とする請求項１記載のコンテンツ管理方法。
【請求項３】　前記コンテンツ毎の少なくとも前記複製可能コンテンツ数を秘匿された特定手続にてアクセス可能な秘匿記憶領域に記録することを特徴とする請求項１記載のコンテンツ管理方法。
【請求項４】　前記コンテンツ毎の少なくとも前記複製可能コンテンツ数と複製コンテンツを記憶した記憶媒体の識別情報とを秘匿された特定手続にてアクセス可能な秘匿記憶領域に記憶し、前記秘匿記憶領域に前記記憶媒体の識別情報が記憶されているときのみ該記憶媒体から該複製コンテンツを消去することを特徴とする請求項１記載のコンテンツ管理方法。
【請求項５】　前記記憶媒体に前記複製コンテンツを記録する際、該記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報と該複製コンテンツの移動の可否を表すフラグ情報とを記録し、該フラグ情報を参照して、該複製コンテンツの移動の可否を判断することを特徴とする請求項１記載のコンテンツ管理方法。
【請求項６】　前記記憶媒体に対するデータの読み出しあるいは書き込み処理にかかる時間が所定時間以内でないとき、以降の処理を中断することを特徴とする請求項１記載のコンテンツ管理方法。
【請求項７】　前記記憶媒体として、その記憶領域内に、秘匿された特定の手続のみにてアクセス可能な秘匿領域が設けられるとともに該記憶媒体の識別情報が記憶された第１の種別の記憶媒体と、前記秘匿領域を具備しないが該記憶媒体の識別情報は有している第２の種別の記憶媒体と、前記秘匿領域および該記憶媒体の識別情報を持たない第３の種別の記憶媒体とがあり、前記記憶媒体に複製コンテンツを記録する際および該記憶媒体から複製コンテンツを消去する際および該記録媒体に記憶された複製コンテンツを再生する際には、該記憶媒体の種別を判別してから、それに応じた処理を施すことを特徴とする請求項１記載のコンテンツ管理方法。
【請求項８】　記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理装置であって、
前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを１つ記録する毎に前記複製可能コンテンツ数から１減算する複製コンテンツ記録手段と、前記記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該複製コンテンツを１つ消去する毎に前記複製可能コンテンツ数を１加算する複製コンテンツ移動手段と、
を具備したことを特徴とするコンテンツ管理装置。
【請求項９】　前記記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報を記録することを特徴とする請求項８記載のコンテンツ管理装置。
【請求項１０】　前記コンテンツ毎の少なくとも前記複製可能コンテンツ数を秘匿された特定手続にてアクセス可能な秘匿記憶領域に記録することを特徴とする請求項８記載のコンテンツ管理装置。
【請求項１１】　前記コンテンツ毎の少なくとも前記複製可能コンテンツ数と複製コンテンツを記憶した記憶媒体の識別情報とを秘匿された特定手続にてアクセス可能な秘匿記憶領域に記憶し、前記秘匿記憶領域に前記記憶媒体の識別情報が記憶されているときのみ該記憶媒体から該複製コンテンツを消去することを特徴とする請求項８記載のコンテンツ管理装置。
【請求項１２】　前記記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報と該複製コンテンツの移動の可否を表すフラグ情報とを記録し、該フラグ情報を参照して、該複製コンテンツの移動の可否を判断することを特徴とする請求項８記載のコンテンツ管理装置。
【請求項１３】　前記記憶媒体に対するデータの読み出しあるいは書き込み処理にかかる時間が所定時間以内でないとき、以降の処理を中断することを特徴とする請求項８記載のコンテンツ管理装置。
【請求項１４】　前記記憶媒体に複製コンテンツを記録する際および該記憶媒体から複製コンテンツを消去する際および該記録媒体に記憶された複製コンテンツを再生する際には、前記記憶媒体が、その記憶領域内に秘匿された特定手続にてアクセス可能な秘匿領域が設けられるとともに該記憶媒体の識別情報が記憶された第１の種別の記憶媒体か、前記秘匿領域を具備しないが該記憶媒体の識別情報は有している第２の種別の記憶媒体か、前記秘匿領域および該記憶媒体の識別情報を持たない第３の

種別の記憶媒体のうちのいずれであるかを判別する判別手段を具備し、この判別手段で判別された前記記録媒体の種別に応じた処理を施すことを特徴とする請求項８記載のコンテンツ管理装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、記憶媒体に記憶できる音楽や映画等の複製コンテンツの数を規制するためのコンテンツ管理方法およびそれを用いたコンテンツ管理装置に関する。

【０００２】

【従来の技術】従来、コンテンツ（著作物等）は、コピー管理が行われてきた。コピー世代管理やコピーの数を管理する事により、著作権保護と利用の便宜のバランスをとってきた。

【０００３】さらに、コピー管理に代わって、「移動」の概念が登場してきた。コピーがオリジナルのデータを消去しないのと対照的に、移動は、異なった場所（メディア）にデータを転送すると共に、オリジナルデータを消去する。コンテンツのデジタル化とネットワーク等の普及が、移動によるコピープロテクションが登場した背景にある。

【０００４】

【発明が解決しようとする課題】近年、ネットワーク等を通じたオリジナルの忠実なコピーが可能になったため、コピー管理だけでは、著作権保護が困難になってきた。また、メディアからメディアへの無制限な移動、例えば、データの営利目的の（移動による）配布は、著作権管理を行うことができない。

【０００５】このように、オリジナルのデータ（特に、著作権保護の対象となるようなコンテンツ）の複製を確実に管理することが困難となってきた。

【０００６】そこで、本発明は、上記問題点に鑑み、記憶媒体に記録できる複製コンテンツの数を規制することによりコンテンツの複製を制限して、コンテンツの著作権を保護することのできるコンテンツ管理方法およびそれを用いたコンテンツ管理装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】１．（請求項１：チェックイン／チェックアウト）本発明のコンテンツ管理方法は、記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法であって、前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを１つ記録する毎に前記複製可能コンテンツ数から１減算し（チェックアウト）、また、該記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該複製コンテンツを１つ消去する毎に前記複製可能コンテンツ数を１加算する（チェックイン）ことを特徴とする。

【０００８】（請求項８）本発明のコンテンツ管理装置は、記憶媒体に記憶できる複製コンテンツの数を規制するためのコンテンツ管理装置であって、前記コンテンツ毎に予め定められた複製可能コンテンツ数を付与し、前記記憶媒体への複製記録指示を受けると、該複製可能コンテンツ数に残数があるとき、該記憶媒体へ前記複製コンテンツを記録し、その際、該記憶媒体に複製コンテンツを１つ記録する毎に前記複製可能コンテンツ数から１減算する複製コンテンツ記録手段と、前記記憶媒体の前記複製コンテンツの消去指示を受けると、該記憶媒体から該複製コンテンツを１つ消去する毎に前記複製可能コンテンツ数を１加算する複製コンテンツ移動手段とを具備したことを特徴とする。

【０００９】本発明によれば、複製コンテンツの数を効率よく規制することができる。

【００１０】２．（請求項２、９：記憶媒体に秘匿領域を設ける）好ましくは、前記記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報（例えば、暗号化されたコンテンツ復号鍵を復号するために必要な乱数ｒ）を記録することを特徴とする。

【００１１】これにより、記憶媒体内の秘匿領域に記録されたデータ（例えば乱数ｒ）は、特定手続（例えば、認証による正当性の確認）が行えない別の記憶媒体に退避する事はできない。従って、例えば「ＴＩＤ１」というコンテンツのチェックイン後、記憶媒体に復帰されたコンテンツを利用する事はできくなるので複製コンテンツ管理のための信頼性が向上する。

【００１２】３．（請求項３、１０：宿帳を秘匿領域に記憶する）好ましくは、前記コンテンツ毎の少なくとも前記複製可能コンテンツ数を秘匿された特定手続にてアクセス可能な秘匿記憶領域に記録することを特徴とする。

【００１３】これにより、秘匿領域に記憶される宿帳（コンテンツ毎の少なくとも複製可能コンテンツ数（子の残数）を登録したもの）は、特定手続（例えば、認証による正当性の確認）が行えない別の記憶媒体に退避する事はできない。従って、例えば「ＴＩＤ１」というコンテンツをチェクアウトした後で、宿帳をチェックアウト前の状態に戻す事はできなくなるので、複製コンテンツ管理のための信頼性が向上する。

【００１４】４．（請求項４、１１：宿帳のチェックアウトリストにのっている記憶媒体のみがチェックイン可）好ましくは、前記コンテンツ毎の少なくとも前記複製可能コンテンツ数と複製コンテンツを記憶した記憶媒体の識別情報とを（宿帳として）秘匿された特定手続にてアクセス可能な秘匿記憶領域に記憶し、前記秘匿記憶

領域に前記記憶媒体の識別情報が記憶されているときのみ該記憶媒体から該複製コンテンツを消去することにより、より厳密に複製コンテンツの管理が行える。

【００１５】５．（請求項５、１２：フラグによるチェックインの制限）好ましくは、前記記憶媒体に前記複製コンテンツを記録する際、該記憶媒体の記憶領域に設けられた秘匿された特定手続にてアクセス可能な秘匿領域に、前記複製コンテンツを再生するために必要な情報と該複製コンテンツの移動の可否を表すフラグ情報とを記録し、該フラグ情報を参照して、該複製コンテンツの移動の可否を判断する。

【００１６】例えば宿帳にない記憶媒体からの複製コンテンツのチェックインを可能にすると、コンテンツの中古市場が成立する原因を作ることにもなる。この対策として、記憶媒体の秘匿領域にチェックインを制限するためのフラグ情報を記録し、複製コンテンツのチェックインを行う際に、まず、当該記憶媒体から読み出したフラグ情報をチェックしてチェックインが可能であるか否かを確認する。そして、可能であると判断されたときのみ、チェックインを行うことにより、コンテンツ毎にチェックインを容易にコントロールできる。

【００１７】６．（請求項６、１３：ネットワークを介する記憶媒体への複製コンテンツの記録を制限）好ましくは、前記記憶媒体に対するデータの読み出しあるいは書き込み処理にかかる時間が所定時間以内でないとき、以降の処理を中断することにより、ネットワークを介した違法な複製コンテンツの配信を未然に防ぐことができ、複製コンテンツの作成をより厳密に規制することができる。

【００１８】７．（請求項７、１４：記憶媒体の種別を判別してからチェックイン、チェックアウト、再生処理を行う）好ましくは、前記記憶媒体として、その記憶領域内に、秘匿された特定の手続のみにてアクセス可能な秘匿領域が設けられるとともに該記憶媒体の識別情報が記憶された第１の種別（レベル２）の記憶媒体と、前記秘匿領域を具備しないが該記憶媒体の識別情報は有している第２の種別（レベル１）の記憶媒体と、前記秘匿領域および該記憶媒体の識別情報を持たない第３の種別（レベル０）の記憶媒体とがあり、前記記憶媒体に複製コンテンツを記録する際および該記憶媒体から複製コンテンツを消去する際および該記録媒体に記憶された複製コンテンツを再生する際には、該記憶媒体の種別を判別してから、それに応じた処理を施すことを特徴とする。

【００１９】これにより、従来からある構成の記憶媒体（レベル０やレベル１）を用いてチェックイン／チェックアウトによる複製コンテンツの管理も容易に行える。

【００２０】

【発明の実施の形態】以下、本発明の実施形態について、図面を参照して説明する。図１は、本実施形態にかかる記憶媒体（メディア）に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法を用いた音楽コンテンツ利用管理システム（以下、簡単にＬＣＭと呼ぶことがある）１の構成例を示したものである。なお、ここでは、コンテンツとして音楽を一例として用いているが、この場合に限らす、映画や、ゲームソフト等であってもよい。また、メディアとしてメモリカード（ＭＣ）を用いているが、この場合に限るものではなく、フロッピー（登録商標）ディスク、ＤＶＤ等の各種記憶媒体であってもよい。

【００２１】ＥＭＤ（Electronic Music Distributor）は、音楽配信サーバまたは音楽配信放送局である。コンテンツ利用管理システム１は、例えば、パソコン（ＰＣ）であり、複数のＥＭＤ（ここでは、ＥＭＤ＃１～＃３）に対応した受信部＃１～＃３を具備しており、ＥＭＤが配信する暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツ復号鍵）などを受信する。受信部＃１～＃３は、再生機能や課金機能を有して居ても良い。配信された音楽コンテンツを試聴する為に再生機能が用いられる。又、課金機能を利用して、気に入ったコンテンツを購入する事が可能である。

【００２２】ＬＣＭ１は、セキュア・コンテンツ・サーバ（ここでは、Secure Music Server：ＳＭＳで、以下、簡単にＳＭＳと呼ぶことがある）２を具備し、利用者が購入したコンテンツはＥＭＤインタフェース（Ｉ／Ｆ）部３を経由してＳＭＳ２に蓄積される。音楽コンテンツは、必要に応じてＥＭＤＩ／Ｆ部３で復号され、形式変換や再暗号化が施される。ＳＭＳ２が暗号化コンテンツを受け取ると、それを音楽データ格納部１０に格納し、音楽データ復号鍵をライセンス格納部９に格納する。ＳＭＳ２が再生機能を有して居ても良い。当該再生機能により、ＳＭＳ２が管理する音楽コンテンツをＰＣ上で再生する事ができる。

【００２３】ＳＭＳ２は、メディア（以下、簡単にＭＣ（memory　card）と呼ぶことがある）１３に対してコンテンツデータを出力する機能を有している。ＭＣ１３を記録再生装置（以下、簡単にＰＤ（Portable Device）と呼ぶことがある）１２にセットし、ＭＣ１３に記録されたコンテンツを再生することができる。

【００２４】ＳＭＳ２からＭＣ１３へのコンテンツの記録はメディア（ＭＣ）インタフェース（Ｉ／Ｆ）部６を通じて直接行われるか、又はＰＤ１２を経由して行うことができる。

【００２５】ＭＣ１３は、そのメディア固有かつ書き換え不能の識別情報（ＭＩＤ）を有しており、ＭＣ１３に格納されるコンテンツは、ＭＣ１３に依存するコンテンツ復号鍵で暗号化される。

【００２６】コンテンツ復号鍵は、メディアＩ／Ｆ部６およびＰＤ１２内部に格納されている暗号鍵Ｋｐによって暗号化され、ＭＣ１３に記録される。

【００２７】ＭＣ１３内のコンテンツ及びコンテンツ復

号鍵は、別個の任意の記憶媒体（以下、ＭＣｂと呼ぶ）にコピーする事が可能であるが、
１．　正統なＰＤ１２のみが暗号鍵Ｋｐを有する事から、ＭＣｂに格納されたコンテンツは正統なＰＤ１２でなければ正しく再生されない。ところが、
２．　ＭＣ１３の識別情報ＭＩＤはコピーできない事から、ＭＣｂの識別情報ＭＩＤはコピー元のＭＣ１３の識別情報ＭＩＤとは異なっており、結局、ＭＣｂにコピーされたコンテンツを正しく再生する事はできない。すなわち、ＳＭＳ２がＭＣ１３に記録した複製コンテンツが、次々と別のＭＣにコピーされ利用される事が防止されている。
【００２８】以上が従来から考えられているＬＣＭ１の構成であるが、次に、本発明にかかる方法および構成部について説明する。
【００２９】まず、チェックイン／チェックアウトについて、図１のＬＣＭ１に則して説明する。
【００３０】チェックアウトとは、ＬＭＳ１が「親」としてのコンテンツを格納しており、ＭＣ１３に、その複製を「子」コンテンツとしてコピーすることをいう。「子」コンテンツはＰＤ１２で自由に再生する事が可能であるが、「子」から「孫」コンテンツを作成する事は許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、ＭＣ１３をＬＣＭ１に接続し、ＬＣＭ１が「子」コンテンツを消去（又は利用不能）する事で、ＬＣＭ１内の「親」コンテンツは「子」を１つ作る権利を回復することをいう。これを「親」にチェックインするともいう。
【００３１】このチェックイン／チェックアウトを単純に、従来からのＬＣＭ１で実現しようとすると、実際、次の様な「攻撃」が存在する。すなわち、ＭＣ１３に格納された「子」を別の記憶メディアに（ＭＩＤを除いて）退避しておき、ＭＣ１３の「子」を「親」にチェックインする。次いで、先に退避しておいた「子」を当該ＭＣ１３に書き戻す。既にチェックインは済んでいるので、ＬＣＭ１上の「親」は別のＭＣ１３に「子」をコピーして良い。この方法で、任意の個数だけ利用可能な「子」を作る事が可能である。
【００３２】上述の「攻撃」には、ＭＣ１３とＬＣＭ１とのデータ転送の際に認証を行う事により、対抗可能である。すなわち、ＭＣ１３は正当なＬＣＭ１以外からのデータ転送を受け付けず、ＬＣＭ１が正当なＭＣ１３以外からのデータ転送を受け付けないと仮定する。この場合、ＭＣ１３内の「子」を別の記録メディアに退避する事はできない。又、ＬＣＭ１に対して、偽って、チェックインすることもできない。従って、上述の「攻撃」は破綻する。
【００３３】ところが、実は、ＬＣＭ１とＭＣ１３との認証を前提としても、チェックイン／チェックアウトは実現できない。次の様な「攻撃」が存在するからである。すなわち、まず、ＬＣＭ１上の「親」が「子」を作っていない状態で、ＬＣＭ１のデータ（特に、ライセンス格納部９の情報）を別の記憶メディアにバックアップする。ＭＣ１３に「子」をコピーした後、バックアップしたＬＣＭ１のデータを復帰する。ＬＣＭ１の「親」は「子」を作る前の状態に戻るから、別のＭＣ１３に「子」を作成する事ができる。この様にして、任意の数の「子」を作成する事が可能となってしまう。
【００３４】次に、チェックイン／チェックアウトを実現する上で生じる問題点以外の問題点について説明する。すなわち、インターネット等の所定の通信路を経由したＭＣ１３への記録である。ＥＭＤによる正規のインターネット配信は、著作権所有者の許諾を得て行う正当な配信であるから問題は無い。ところが、図２１の様な形態で、インターネット経由でＭＣ１３へのコンテンツの記録を行う事ができてしまう。図２１におけるパソコン（ＰＣ）上の通信部２０１は、単にＭＣ１３への書き込みプロトコルを中継しているだけである。ＬＣＭ１は、当該ＬＣＭ１が稼働するＰＣ＃２に直接接続されているＰＤ１２と、通信部２０１を介してリモート接続されているＬＣＭ１の稼働するＰＣ＃２に接続されているＰＤ１２とを区別する事ができない為、インターネット等のネットワークを介したコンテンツの（違法な）配布が可能である。
【００３５】以下、本発明の要旨である、チェックイン／チェックアウトと、ネットワークを介するＭＣ１３へのコンテンツ記録を規制するための手段等について、次に示す項目の順に説明する。
【００３６】１．チェックイン／チェックアウト
（１－１）チェックイン／チェックアウト
（１－２）レベル２のＭＣを用いた複製コンテンツのチェックイン／チェックアウト
（１－３）宿帳による複製コンテンツの他の管理方法
（１－４）レベル２のＭＣに記憶された複製コンテンツの再生
（１－５）レベル１のＭＣを用いた複製コンテンツのチェックイン／チェックアウト、複製コンテンツの再生
（１－６）レベル０のＭＣを用いた複製コンテンツのチェックイン／チェックアウト、複製コンテンツの再生
２．ネットワークを介するＭＣへの複製コンテンツの記録を規制するための手段
３．秘匿領域
（チェックイン／チェックアウト）チェックイン／チェックアウトを実現するために、ＭＣ１３内の記憶領域に、公開された手順では読み書きできない領域（秘匿領域）を設け、そこにコンテンツ復号に必要な情報を記録する（図２参照）。また、ＬＣＭ１の記憶領域（例えば、ＬＣＭ１がＰＣで構成されている場合には、ハードディスク（ＨＤＤ））上に非公開の手順でしかアクセス

できない領域（秘匿領域）を設け、後述するような宿帳を当該秘匿領域に格納する（図２参照）。さらに、ＰＤ１２の記憶領域上にも非公開の手順でしかアクセスできない領域（秘匿領域）を設け、そこにコンテンツ復号に必要な情報を記録するようにしてもよい（図２参照）。なお、ここでは、記憶領域中の秘匿領域以外の通常に手順にてアクセス可能な領域を公開領域と呼ぶ。

【００３７】図１に示すように、ＬＣＭ１では、秘匿領域には、宿帳格納部８が設けられ、ＳＭＳ２にてこの宿帳格納部８にアクセスするための秘匿された特定の手続が行われた後、秘匿領域からデータを読み取るための秘匿領域ドライバ７を具備している。

【００３８】図４（ｃ）に示すように、ＭＣ１３は、その識別情報ＭＩＤを格納するための外部からは書換不可能で、コピーも不可能なような構成になっている識別情報格納部１３ｂと、秘匿領域１３ｃと、公開領域１３ａと、秘匿領域１３ｃにアクセスされる度に認証部１３ｄにて認証を行って、正当な相手であると確認されたときに初めて秘匿領域１３ｃにアクセス可能なようにゲートを開くスイッチ（ＳＷ）１３ｅを具備する。なお、本実施形態で利用可能なＭＣ１３は、３種類あり、図４（ｃ）に示すような、識別情報ＭＩＤと秘匿領域とを両方兼ね備えているＭＣ１３の種別を「レベル２」と呼ぶ。秘匿領域は持たないが識別情報ＭＩＤは持つ図４（ｂ）に示すようなＭＣ１３の種別を「レベル１」と呼ぶ。秘匿領域も識別情報も持たない図４（ａ）に示すようなＭＣ１３の種別を「レベル０」と呼ぶことにする。これら種別は、例えば、識別情報ＭＩＤの有無でレベル０とそれ以外の種別とが判別でき、さらに、識別情報ＭＩＤの構成からレベル１とレベル２とを判別する。例えば、識別情報が連続した数値であるとき、所定値以上はレベル２であるとする。

【００３９】以下、特に断らない限り、レベル２のＭＣ１３の場合を例にとり説明する。

【００４０】このＭＣ１３は、ＬＣＭ１に接続されたＰＤ１２にセットして用いる場合とＬＣＭ１に直接セットして用いる場合とがある。

【００４１】図３は、ＰＤ１２の構成例を示したもので、ＭＣ１３は、メディアインタフェース（Ｉ／Ｆ部）１２ｆにセットされる。ＬＣＭ１がＰＤ１２を介してＭＣ１３に読み書きする場合は、ＰＤ１２内の秘匿領域アクセス部を経由してＭＣ１３の秘匿領域にアクセスする。メディアＩ／Ｆ部１２ｆには、ＭＣ１３の秘匿領域にアクセスするための秘匿領域アクセス部を具備している。ＰＤ１２内の秘匿領域は、フラッシュメモリ１２ｄに設けれていても良い。ＲＯＭ１２ｃには、ＭＣ１３との間で相互認証を行うためのプログラムや、ＭＣ１３の種別を判別するためのプログラムも書き込まれていて、このプログラムに従って、ＣＰＵ１２ａの制御の下、ＭＣ１３との間の相互認証、種別判別等の処理を実行するようになっている。

【００４２】図５は、ＬＣＭ１のメディアＩ／Ｆ部６の構成を示したもので、ＭＣ１３との間で相互認証を行うための認証部６ｃと、ＭＣ１３の種別を判別するメディア判別部６ｂと、これら全体を制御するための制御部６ａとから構成されている。認証部６ｃは、ＭＣ１３の秘匿領域にアクセスするための秘匿領域アクセス部である。

【００４３】次に、ＬＣＭ１の秘匿領域に格納される宿帳について説明する。

【００４４】ＳＭＳ２にて保持する全ての音楽コンテンツは、そのそれぞれを識別するための識別情報であるコンテンツＩＤ（ＴＩＤ）と、予め定められた複製可能コンテンツ数、すなわち、子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼ぶ。宿帳は、秘匿領域に設けられた宿帳格納部８に図７（ａ）に示すような形態で記録されている。

【００４５】図７（ａ）において、例えば、コンテンツＩＤ「ＴＩＤ１」なる子の残数は「２」で、そのチェックアウトリストはＬ１である。

【００４６】チェクアウトリストは、複製コンテンツ（子）を記録したＭＣ１３の識別情報のリストであって、例えば、図７（ａ）において、チェックアウトリストＬ１には「ｍ１」と「ｍ２」という識別情報を持つ２つのＭＣ１３にコンテンツＩＤ「ＴＩＤ１」なるコンテンツの子がチェックアウトされていることがわかる。

【００４７】（レベル２のＭＣを用いた複製コンテンツのチェックイン／チェックアウト）次に、図４（ｃ）に示したような構成のレベル２のＭＣ１３を用いたチェックイン／チェックアウトについて、図９～図１１を参照して説明する。

【００４８】ＭＣ１３がＬＣＭ１のメディアＩ／Ｆ部６、あるいは、ＰＤ１２にセットされると、メディアＩＦ部６とＭＣ１３との間、あるいは、ＰＤ１２とＭＣ１３との間で相互認証が行われ（図９のステップＳ１）、双方にて正当な相手であると判断されたとき（ステップＳ２）、メディアＩ／Ｆ部６あるいはＰＤ１２はＭＣ１３から読み取った識別情報ＭＩＤを基に、ＭＣ１３の種別を判別する（ステップＳ３）。ここでは、ＭＣ１３の種別は、レベル２であるので、メディアＩ／Ｆ部６あるいはＰＤ１２は、その種別に応じたチェックイン／チェックアウト処理を実行する（ステップＳ６）。

【００４９】チェックアウトの指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介して、あるいは、ＰＤ１２を介して、ＳＭＳ２になされた場合について、図１０を参照して説明する。ＳＭＳ２は、宿帳のチェックアウト要求のあったコンテンツ（例えばコンテンツＩＤが「ＴＩＤ１」であるとする）の子の残数ｎを調べ（ステップＳ１０１）、ｎ＞０のとき、必要があれば、ＭＣ１３との間で相互認証を行い（ステップＳ１０

２）、相互に正当性が確認されたら、次に、ＭＣ１３から、その識別情報ＭＩＤ（例えば、ＭＩＤ＝ｍ０とする）を転送してもらう（ステップＳ１０３）。

【００５０】ＳＭＳ２では、乱数ｒを発生し、この乱数ｒと、ＭＣ１３の識別情報ｍ０と、正当なるＭＣ１３とＬＣＭ１との間で共有する鍵生成アルゴリズムＷと用いて、暗号化鍵ｗを生成する。なお、鍵生成アルゴリズムＷは、２つの引数（ここでは、ｒとｍ０）をとり、暗号化鍵ｗを毎回変化させる役割を果たす。さらに、ＳＭＳ２では、暗号化されたコンテンツを復号するためのコンテンツ復号鍵Ｋ（Ｃ）をＭＣ１３とＬＣＭ１との間で共有する暗号鍵Ｋｐと先に生成した暗号化鍵ｗとで暗号化する。それをｗ［Ｋｐ［ｋ（Ｃ）］］と表す。また、コンテンツＣを鍵Ｋ（Ｃ）で暗号化する。それをＫ（Ｃ）［Ｃ］と表す（ステップＳ１０４）。

【００５１】ＳＭＳ２は、ＭＣ１３の記憶領域に、例えば「ＴＩＤ１」という名前のフォルダを作成すると（ステップＳ１０５）、当該フォルダの公開領域に暗号化されたコンテンツＫ（Ｃ）［Ｃ］と、暗号化されたコンテンツ復号鍵ｗ［Ｋｐ［ｋ（Ｃ）］］とを書き込む（ステップＳ１０６、ステップＳ１０７）。

【００５２】次に、ＳＭＳ２は、ＭＣ１３の秘匿領域１３ｃにアクセスすべく、ＭＣ１３との間で相互認証を行い、双方の正当性が確認されてスイッチ１３ｅにより秘匿領域１３ｃへのゲートが開かれると、乱数ｒを秘匿領域１３ｃ内のフォルダ「ＴＩＤ１」に対応する領域に書き込む（ステップＳ１０８～ステップＳ１０９）。それが終了すると秘匿領域１３ｃへのアクセスを可能にしていたゲートがスイッチ１３ｅにより閉じられる仕組みになっている。また、ステップＳ１０８において、乱数ｒを秘匿領域１３ｃに転送するまでの経路は、乱数ｒを暗号化する等して転送保護することが望ましい。

【００５３】最後に、ＳＭＳ２は、図７（ｂ）に示すように、宿帳のチェックアウト要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎから「１」減算し、チェックアウトリストＬ１に、当該ＭＣ１３の識別情報「ｍ０」を追加する（ステップＳ１１０）。

【００５４】以上の処理が終了したときのＭＣ１３の記憶内容を図６に示す。

【００５５】チェックインの指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介して、あるいは、ＰＤ１２を介して、ＳＭＳ２になされた場合について、図１１を参照して説明する。

【００５６】ＳＭＳ２は、必要があれば、ＭＣ１３との間で相互認証を行い（ステップＳ２０１）、相互に正当性が確認されたら、次に、ＭＣ１３から、その識別情報ＭＩＤ（例えば、ＭＩＤ＝ｍ０とする）を転送してもらう（ステップＳ２０２）。

【００５７】ＳＭＳ２は、チェックイン要求のなされたコンテンツ（例えばコンテンツＩＤが「ＴＩＤ１」であるとする）の宿帳から、そのチェックアウトリストに当該ＭＣ１３の識別情報、すなわち、ここでは、「ｍ０」が登録されているとき、乱数ｒ１、ｒ２を発生させる（ステップＳ２０３）。そして、ＭＣ１３の公開領域１３ａの当該コンテンツのフォルダ（ここでは、フォルダ「ＴＩＤ１」）に対応する領域に記憶されている情報を乱数ｒ２で上書きすることで消去し（ステップＳ２０４）、また、ＳＭＳ２は、ＭＣ１３の秘匿領域１３ｃにアクセスすべく、ＭＣ１３との間で相互認証を行い、双方の正当性が確認されてスイッチ１３ｅにより秘匿領域１３ｃへのゲートが開かれると、秘匿領域１３ｃ内のフォルダ「ＴＩＤ１」に対応する領域を乱数ｒ１で上書きすることで消去する（ステップＳ２０５）。それが終了すると秘匿領域１３ｃへのアクセスを可能にしていたゲートがスイッチ１３ｅにより閉じられる仕組みになっている。また、ステップＳ２０５において、乱数ｒ１を秘匿領域１３ｃに転送するまでの経路は、乱数ｒ１を暗号化する等して転送保護することが望ましい。

【００５８】その後、ＳＭＳ２では、上書き消去の確認をすべく、ＭＣ１３から上書き後の各領域の値を転送してもらい（ステップＳ２０６）、それが数ｒ１、ｒ２と一致するかどうかチェックする（ステップＳ２０７）。上書き消去の確認がなされたら、ＭＣ１３からフォルダ「ＴＩＤ１」を消去する（ステップＳ２０８）。

【００５９】最後に、図７（ｃ）に示すように、宿帳のチェックイン要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎに「１」加算し、チェックアウトリストＬ１から、当該ＭＣ１３の識別情報ｍ０を削除する（ステップＳ２０９）。

【００６０】ＭＣ１３内の秘匿領域１３ｃに記録された乱数ｒは、（認証による正当性が確認できないので）別の記憶メディアに退避する事はできない。従って、「ＴＩＤ１」というコンテンツのチェックイン後、ＭＣ１３に復帰されたコンテンツを利用する事はできない。又、ＬＣＭ１の秘匿領域にて記憶される宿帳も（認証による正当性が確認できないので）別の記録メディアに退避する事ができない。従って、「ＴＩＤ１」というコンテンツをチェクアウトした後で、宿帳をチェックアウト前の状態に戻す事はできない。この様に、本発明は先述の攻撃に対する対策を提供する。

【００６１】なお、チェックインの際、ＭＣ１３の秘匿領域の内容を乱数で上書きする事は、セキュリティ上重要である。ＭＣ１３の秘匿領域に書き込みを行い得るのは、正統なＳＭＳ２のみであるが、逆に正統なＳＭＳ２は、必ず秘匿手続きによって秘匿領域に書き込みを行う。秘匿手続きによる書き込みが成功する事を以って、ＭＣ１３の正統性が保証される。即ち、不正なチェックインを防止する事が可能である。安全性を高めるため、ＳＭＳ２は秘匿領域を任意の乱数で上書きした後、その内容を（秘匿手続きによって）読み込み、上書きした乱

数である事を確認する様にしている。

【００６２】（宿帳による複製コンテンツの他の管理方法）なお、ＳＭＳ２は、宿帳に無いタイトル（コンテンツＩＤ）のコンテンツをチェックインする様にしても良い。又、チェックアウトリストに無いＭＣ１３からのチェックインを認めても良い。この場合、宿帳は、各コンテンツに対するチェックアウトリストを持たない。チェックアウトリストは、「身に覚えの無い」ＭＣ１３からのチェックインを防止するために参照されるものだからである。この場合の宿帳の記憶内容を図８（ａ）に示す。

【００６３】図８（ａ）に示すように、各コンテンツの宿帳には、そのコンテンツＩＤと子の残数のみが登録されている。

【００６４】今、ＴＩＤ７と言うコンテンツＩＤを有するコンテンツを、メディア識別情報ＭＩＤ＝ｍ０を有するＭＣ１３からチェックインする場合を考える。すなわち、当該ＭＣ１３には、現在、別のＳＭＳ２からチェックアウトされたコンテンツＩＤ「ＴＩＤ７」なるコンテンツが、図６に示したような形態で記憶されている。

【００６５】ＬＣＭ１は、図１１に示した手続のうち、ステップＳ２０３のチェックアウトリストの参照を行わずにＭＣ１３内の秘匿領域、公開領域の記憶内容を消去するとともに、フォルダ「ＴＩＤ７」を削除する。そして、宿帳に新たなコンテンツの宿帳（ＴＩＤ７、１）を登録する。

【００６６】ＬＣＭ１が宿帳に無いコンテンツをチェックインする事で、例えば次の様な事が可能になる。自宅ＰＣにて構成されるＬＣＭ１が格納する「親」コンテンツが「子」を２つ持つ事ができるとする。自宅ＰＣからＭＣ１３に「子」を１つチェックアウトし、友人宅のＰＣにチェックインする。自分が購入した「親」が「子」を作る数を１つ減らして、友人にコンテンツをプレゼントした事になる。

【００６７】このように、ＬＣＭ１が宿帳にないコンテンツのチェックインを可能とすると、「子」のコンテンツがＬＣＭ１を介して「移動」する事が可能である。これはユーザにとっては便利な機能であるが、コンテンツの中古市場が成立する原因を作ることにもなる。実際、次のような中古コンテンツ売買が成立する。すなわち、ユーザがＥＭＤから新作のコンテンツを購入し、短期間所持した後に、中古データ販売店のＬＣＭ１に当該コンテンツをチェックインする。この際、当該ユーザは代金を受け取る。中古データ販売店は、別の購入希望者に、ＥＭＤの正規価格より安い値段でデータを販売する。

【００６８】この様に、コンテンツの著作権をコントロールできない「中古市場」の成立は、コピーライト・ホルダーにとって好ましくない。従って、コピーライト・ホルダーが、異なったＬＣＭ１へのチェックインをコントロールできる様、各コンテンツにチェックアウト属性フラグｆを持たせても良い。

【００６９】この場合のＬＣＭ１が有する宿帳の形式を図１８（ａ）に示す。

【００７０】図１８（ａ）に示すように、各コンテンツの宿帳には、そのコンテンツＩＤと子の残数とチェックアウトリストとチェックアウト属性フラグｆが登録されている。

【００７１】フラグｆが「１」の場合、当該コンテンツは他のＬＣＭ１にチェックアウト、チェックイン可能であるが、フラグｆが「０」のときは、当該コンテンツは、少なくとも他のＬＣＭ１にチェックインするこはできない。

【００７２】例えば、コンテンツＩＤ「ＴＩＤ６」というコンテンツをチェックアウトする場合を考える。まずＳＭＳ２は宿帳を調べ、当該コンテンツのチェックアウト属性フラグが「１」であることを確認する。ここでは、この値が「０」であるとき、当該ＬＣＭ１では、当該コンテンツをチェックアウトしないこととする。フラグｆが「１」であるときは、図１０に示した手順と同様にして、コンテンツＩＤ「ＴＩＤ６」の宿帳の子の残数から「１」減算して「１」とする（図１８（ｂ）参照）。ちなみに、チェックアウトリストＬ６は空（φと表記する）であり、しかもフラグｆは「１」であり、当該コンテンツは他のＰＣ上の設けられたＬＣＭ１にチェックイン可能であるから、チェックアウトリストを持つ必要がない。また、フラグｆは、ＭＣ１３の秘匿領域に乱数ｒとともに記録されるものとする。

【００７３】次に、コンテンツＩＤ「ＴＩＤ６」というコンテンツを、チェックアウトしたＬＣＭ１と同じＬＣＭ１、あるいは別のＬＣＭ１に、チェックインする場合について、図１９に示すフローチャートを参照して説明する。

【００７４】図１１に示した手順にて、ＭＣ１３とＬＣＭ１との間で相互認証を行い（ステップＳ１１）、ＭＣ１３の識別情報ＭＩＤを取得する（ステップＳ１２）。

【００７５】ＳＭＳ２は、チェックイン要求のあったコンテンツが宿帳に登録されているいないにかかわらず、ＭＣ１３の秘匿領域１３ｃに前述した秘匿手続（ＭＣ１３との間で相互認証を行い、双方の正当性が確認されてスイッチ１３ｅにより秘匿領域１３ｃへのゲートが開かれる）を行って、秘匿領域１３ｃからフラグｆを読み取る（ステップＳ１３）。フラグｆが「１」であるときは（ステップＳ１４）、図１１のステップＳ２０４～ステップＳ２０８を行い（ステップＳ１５～１６）、フラグｆが「０」のときは、処理を終了する。そして、最後に、宿帳に当該コンテンツが登録されていないときは、そのコンテンツの子の残数を「１」とした「ＴＩＤ６」の新たな宿帳（ＴＩＤ６、１、φ、１）を登録し、宿帳に当該コンテンツが登録されているときは、そのコンテンツの子の残数に「１」を加算する（ステップＳ１

７）。
【００７６】（レベル２のＭＣに記憶された複製コンテンツの再生）次に、図４（ｃ）に示したような構成のレベル２のＭＣ１３に記憶された複製コンテンツの再生について、図１２を参照して説明する。ＭＣ１３をＰＤ１２にセットすると、ＰＤ１２は、ＭＣ１３から、その識別情報ＭＩＤ（例えば、ＭＩＤ＝ｍ０とする）を転送してもらう（ステップＳ３０１）。このとき、識別情報ＭＩＤ＝ｍ０を基に、ＭＣ１３の種別を判別が、レベル２であることが判別できる。そこで、ＰＤ１２は、ＭＣ１３の公開領域からｗ［Ｋｐ［ｋ（Ｃ）］］を読み出すとともに（ステップＳ３０２）、ＭＣ１３の秘匿領域１３ｃにアクセスすべく、ＭＣ１３との間で相互認証を行い、双方の正当性が確認されてスイッチ１３ｅにより秘匿領域１３ｃへのゲートが開かれると、秘匿領域１３ｃ内のフォルダ「ＴＩＤ１」に対応する領域から乱数ｒを読み出す（ステップＳ３０３）。それが終了すると秘匿領域１３ｃへのアクセスを可能にしていたゲートがスイッチ１３ｅにより閉じられる仕組みになっている。
【００７７】ＰＤ１２は、乱数ｒと、ＭＣ１３の識別情報ｍ０と、正当なるＭＣ１３とＰＤ１２との間で共有する鍵生成アルゴリズムＷと用いて、暗号化鍵ｗを生成する。暗号化鍵ｗと、ＭＣ１３とＬＣＭ１との間で共有する暗号鍵Ｋｐと、ＭＣ１３から読み出されたｗ［Ｋｐ［ｋ（Ｃ）］］とからコンテンツ復号鍵Ｋ（Ｃ）を復号する（ステップＳ３０４）。
【００７８】そして、ＰＤ１２は、ＭＣ１３の公開領域から暗号化されたコンテンツＫ（Ｃ）［Ｃ］を読み出し（ステップＳ３０５）、復号部１２ｇでコンテンツＣを復号し、デコーダ１２ｈでデコードして、Ｄ／Ａ変換部でデジタル信号からアナログ信号に変換し、音楽を再生する（ステップＳ３０６）。
【００７９】（レベル１のＭＣを用いた複製コンテンツのチェックイン／チェックアウト、複製コンテンツの再生）次に、図４（ｂ）に示したような構成のレベル２のＭＣ１３を用いたチェックイン／チェックアウトについて、図９、図１３を参照して説明する。なお、レベル１のＭＣ１３は、秘匿領域を持たないので、チェックインを行うことができない。
【００８０】ＭＣ１３がＬＣＭ１のメディアＩ／Ｆ部６、あるいは、ＰＤ１２にセットされてから、ＭＣ１３の種別が判別されるまでは、図９と同様である。
【００８１】ここでは、ＭＣ１３の種別は、レベル１であるので、メディアＩ／Ｆ部６あるいはＰＤ１２は、その種別に応じたチェックイン／チェックアウト処理を実行する（ステップＳ５）。
【００８２】チェックインの指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介して、あるいは、ＰＤ１２を介して、ＳＭＳ２になされた場合、ＭＣ１３の種別がレベル１であると判別されているので、その指示は、拒否される。
【００８３】チェックアウトの指示がＬＣＭ１のユーザインタフェース（Ｉ／Ｆ）部１５を介して、あるいは、ＰＤ１２を介して、ＳＭＳ２になされた場合について、図１３を参照して説明する。
【００８４】ＳＭＳ２は、宿帳のチェックアウト要求のあったコンテンツ（例えばコンテンツＩＤが「ＴＩＤ１」であるとする）の子の残数ｎを調べ（ステップＳ４０１）、ｎ＞０のとき、必要があれば、ＭＣ１３との間で相互認証を行い（ステップＳ４０２）、相互に正当性が確認されたら、次に、ＭＣ１３から、その識別情報ＭＩＤ（例えば、ＭＩＤ＝ｍ０とする）を転送してもらう（ステップＳ４０３）。
【００８５】ＳＭＳ２は、レベル２の場合と同様、乱数ｒの発生、暗号化鍵ｗの生成、コンテンツ鍵をｗとＫｐを用いて暗号化、コンテンツＣの暗号化を行い（ステップＳ４０４）、ＭＣ１３の記憶領域（ここでは、公開領域のみ）に、例えば「ＴＩＤ１」という名前のフォルダを作成する（ステップＳ４０５）。そして、当該フォルダに暗号化されたコンテンツＫ（Ｃ）［Ｃ］と、暗号化されたコンテンツ復号鍵ｗ［Ｋｐ［ｋ（Ｃ）］］と乱数ｒとを書き込む（ステップＳ４０６～ステップＳ４０８）。
【００８６】最後に、ＳＭＳ２は、図７（ｂ）に示すように、宿帳のチェックアウト要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎから「１」減算し、チェックアウトリストＬ１に、当該ＭＣ１３の識別情報「ｍ０」を追加する（ステップＳ４０９）。
【００８７】次に、レベル１のＭＣ１３に記憶された複製コンテンツの再生について、図１４を参照して説明する。ＭＣ１３をＰＤ１２にセットすると、ＰＤ１２は、ＭＣ１３から、その識別情報ＭＩＤ（例えば、ＭＩＤ＝ｍ０とする）を転送してもらう（ステップＳ５０１）。このとき、識別情報ＭＩＤ＝ｍ０を基に、ＭＣ１３の種別を判別が、レベル１であることが判別できる。そこで、ＰＤ１２は、ＭＣ１３の記憶領域（公開領域のみ）からｗ［Ｋｐ［ｋ（Ｃ）］］、乱数ｒを読み出し（ステップＳ５０２～ステップＳ５０３）、乱数ｒと、ＭＣ１３の識別情報ｍ０と、正当なるＭＣ１３とＰＤ１２との間で共有する鍵生成アルゴリズムＷと用いて、暗号化鍵ｗを生成する。暗号化鍵ｗと、ＭＣ１３とＬＣＭ１との間で共有する暗号鍵Ｋｐと、ＭＣ１３から読み出されたｗ［Ｋｐ［ｋ（Ｃ）］］とからコンテンツ復号鍵Ｋ（Ｃ）を復号する（ステップＳ５０４）。
【００８８】そして、ＰＤ１２は、ＭＣ１３の記憶領域（公開領域のみ）から暗号化されたコンテンツＫ（Ｃ）［Ｃ］を読み出し（ステップＳ５０５）、復号部１２ｇでコンテンツＣを復号し、デコーダ１２ｈでデコードして、Ｄ／Ａ変換部でデジタル信号からアナログ信号に変換し、音楽を再生する（ステップＳ５０６）。

【００８９】（レベル０のＭＣを用いた複製コンテンツのチェックイン／チェックアウト、複製コンテンツの再生）次に、図４（ａ）に示したような構成のレベル０のＭＣ１３を用いたチェックイン／チェックアウトについて、図９、図１５～図１６を参照して説明する。

【００９０】レベル０のＭＣ１３は、ＰＤ１２を用いてしかチェックイン／チェックアウトおよび再生が行えない。また、識別情報ＭＩＤを持たないため、代わりにチェックイン／チェックアウトにおいて、ＰＤ１２の識別情報ＰＩＤが用いられる。

【００９１】ＭＣ１３がＰＤ１２にセットされてから、ＭＣ１３の種別が判別されるまでは、図９と同様である。

【００９２】ここでは、ＭＣ１３の種別は、レベル０であるので、ＰＤ１２は、その種別に応じたチェックイン／チェックアウト処理を実行する（ステップＳ４）。

【００９３】チェックアウトの指示がＰＤ１２を介して、ＳＭＳ２になされた場合について、図１５を参照して説明する。

【００９４】ＳＭＳ２は、宿帳のチェックアウト要求のあったコンテンツ（例えばコンテンツＩＤが「ＴＩＤ１」であるとする）の子の残数ｎを調べ（ステップＳ６０１）、ｎ＞０のとき、ＰＤ１２との間で相互認証を行い（ステップＳ６０２）、相互に正当性が確認されたら、次に、ＰＤ１２から、その識別情報ＰＩＤを転送してもらう（ステップＳ６０３）。

【００９５】ＳＭＳ２は、レベル２の場合と同様、乱数ｒの発生、暗号化鍵ｗの生成、コンテンツ鍵をｗとＫｐを用いて暗号化、コンテンツＣの暗号化を行う（ステップＳ６０４）。但し、ここでは、鍵生成アルゴリズムＷのとる２つの引数は、ｒとＰＩＤである。

【００９６】次に、ＭＣ１３の記憶領域（ここでは、公開領域のみ）に、例えば「ＴＩＤ１」という名前のフォルダを作成する（ステップＳ６０５）。そして、当該フォルダに暗号化されたコンテンツＫ（Ｃ）［Ｃ］と、暗号化されたコンテンツ復号鍵ｗ［Ｋｐ［ｋ（Ｃ）］］を書き込む（ステップＳ６０６～ステップＳ６０７）。乱数ｒは、ＰＤ１２の秘匿領域に書き込む（ステップＳ６０８）。ステップＳ６０８において、乱数ｒをＰＤ１２の秘匿領域に転送するまでの経路は、乱数ｒを暗号化する等して転送保護することが望ましい。

【００９７】最後に、ＳＭＳ２は、図７（ｂ）に示すように、宿帳のチェックアウト要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎから「１」減算し、チェックアウトリストＬ１に、ＰＤ１２の識別情報「ＰＩＤ」を追加する（ステップＳ６０９）。

【００９８】チェックインの指示がＰＤ１２を介して、ＳＭＳ２になされた場合について、図１６を参照して説明する。

【００９９】ＳＭＳ２は、ＰＤ１２との間で相互認証を行い（ステップＳ７０１）、相互に正当性が確認されたら、次に、ＰＤ１２から、その識別情報ＰＩＤを転送してもらう（ステップＳ７０２）。

【０１００】ＳＭＳ２は、チェックイン要求のなされたコンテンツ（例えばコンテンツＩＤが「ＴＩＤ１」であるとする）の宿帳から、そのチェックアウトリストに当該ＰＤ１２の識別情報「ＰＩＤ」が登録されているとき、乱数ｒ１、ｒ２を発生させる（ステップＳ７０３）。そして、ＭＣ１３の公開領域１３ａの当該コンテンツのフォルダ（ここでは、フォルダ「ＴＩＤ１」）に対応する領域に記憶されている情報を乱数ｒ２で上書きすることで消去し（ステップＳ７０４）、また、ＳＭＳ２は、ＰＤ１２の秘匿領域にアクセスすべく、ＰＤ１２との間で相互認証を行い、双方の正当性が確認されて秘匿領域へのゲートが開かれると、秘匿領域１３ｃ内のフォルダ「ＴＩＤ１」に対応する領域を乱数ｒ１で上書きすることで消去する（ステップＳ７０５）。それが終了すると秘匿領域へのアクセスを可能にしていたゲートが閉じられる。また、ステップＳ７０５において、乱数ｒ１を秘匿領域に転送するまでの経路は、乱数ｒ１を暗号化する等して転送保護することが望ましい。

【０１０１】その後、ＳＭＳ２では、上書き消去の確認をすべく、ＭＣ１３から上書き後の値を転送してもらい、また、ＰＤ１２の秘匿領域からも上記所定の秘匿手続を行って、当該領域の上書き後の値を読み出し（ステップＳ７０６）、それが乱数ｒ１、ｒ２と一致するかどうかチェックする（ステップＳ７０７）。上書き消去の確認がなされたら、ＭＣ１３からフォルダ「ＴＩＤ１」を消去する（ステップＳ７０８）。

【０１０２】最後に、図７（ｃ）に示すように、宿帳のチェックイン要求のあったコンテンツＩＤ「ＴＩＤ１」のコンテンツの子の残数ｎに「１」加算し、チェックアウトリストＬ１から、ＰＤ１２の識別情報「ＰＩＤ」を削除する（ステップＳ７０９）。

【０１０３】次に、レベル０のＭＣ１３に記憶された複製コンテンツの再生について、図１７を参照して説明する。ＭＣ１３をＰＤ１２にセットすると、ＰＤ１２は、ＭＣ１３から、その識別情報ＭＩＤの転送を要求するが、ＭＣ１３は、識別情報をもっていないので、ＰＤ１２は、当該ＭＣ１３は、レベル０であると判別できる。そこで、ＰＤ１２は、ＭＣ１３の記憶領域（公開領域のみ）からｗ［Ｋｐ［ｋ（Ｃ）］］を読み出し（ステップＳ８０１）、ＰＤ１２自身の識別情報「ＰＩＤ」と、その秘匿領域に格納されている乱数ｒと鍵生成アルゴリズムＷとを用いて、暗号化鍵ｗを生成する。そして、暗号化鍵ｗと、暗号鍵Ｋｐと、ＭＣ１３から読み出されたｗ［Ｋｐ［ｋ（Ｃ）］］とからコンテンツ復号鍵Ｋ（Ｃ）を復号する（ステップＳ８０２）。

【０１０４】ＰＤ１２は、ＭＣ１３の記憶領域（公開領域のみ）から暗号化されたコンテンツＫ（Ｃ）［Ｃ］を

読み出し（ステップＳ８０３）、復号部１２ｇでコンテンツＣを復号し、デコーダ１２ｈでデコードして、Ｄ／Ａ変換部でデジタル信号からアナログ信号に変換し、音楽を再生する（ステップＳ８０４）。

【０１０５】（ネットワークを介するＭＣへの複製コンテンツ記録を規制するための手段）本発明の２つ目の問題点を解決するために、すなわち、ネットワークを経由したコンテンツのＭＣ１３への記録を規制するために、本発明では、図１に示すようにタイムアウト判定部４を設けている。

【０１０６】タイムアウト判定部４では、ＭＣ１３への読み書き（いずれか一方、又は両方）手順において、一定の制限時間を設定し、処理が制限時間内に終わらなければ処理を中断する。ネットワークを通じた通信は通常、直接接続された機器との通信に比較して遙かに長い時間を要する為、タイムアウト機能によって、ネットワークを通じた違法コピーに対抗する事ができる。又、帯域制限を用いる事もできる。機器との通信帯域を一定以上と仮定すれば、或るサイズのデータを機器に転送する際に要する時間の上限が計算できる。実際の転送時間が、それを上回った場合、処理を中断する。

【０１０７】図２２に示すタイムアウト判定部４の構成と図２３に示すフローチャートを参照して、もう少し具体的に述べる。予めタイムアウト時間をｔと設定することにし、例えば、ＬＣＭ１とＰＤ１２との間の通信帯域幅をｂとする。例えば、ＰＤ１２にセットされているＭＣ１３との間でチェックアウトを行う場合を例にとり、タイムアウト判定部４の処理動作について説明する。

【０１０８】まず、ＰＤ１２にセットされているＭＣ１３との間のチェックアウトのための手順にあるある１つの読み書き処理動作の開始とともに、ＳＭＳ２から判定開始信号入力部１０２を介して判定開始信号が入力し（ステップＳ２０）、それとともに、ＳＭＳ２からＰＤ１２との間でやりとりされるパケットデータのサイズｓがデータサイズ入力部１０１から入力し（ステップＳ２１）、制御部１０５は、時刻取得部１０６を介して時計１０７から現在時刻Ｔを取得する（ステップＳ２２）。これに伴って、帯域幅格納部１０８から帯域幅ｂを取得し（ステップＳ２３）、終了予定時刻Ｔ’を算出して（ステップＳ２４）。最終予定時刻格納部１１１に格納する（ステップＳ２５）。

【０１０９】終了予定時刻Ｔ’は、帯域幅ｂとデータサイズｓとから　Ｔ’＝Ｔ＋ｓ／ｂより求めることができる。

【０１１０】ＰＤ１２にセットされているＭＣ１３との間の読み書き処理動作の終了とともに、ＳＭＳ２から判定終了信号入力部１０３を介して判定終了信号が入力されると（ステップＳ２６）、再び、現在時刻Ｔを取得し（ステップＳ２７）、先に算出された終了予定時刻Ｔ’と現在時刻Ｔとの差とタイムアウト時間ｔとを比較する（ステップＳ２８）。当該差がタイムアウト時間ｔを超えているときは、「ＮＧ」と判定し、その旨をＳＭＳ２へ通知する（ステップＳ３０）。もし、ＰＤ１２が図２１に示したようにチェックアウトを行うＰＣ＃１にあるＬＣＭ１とネットワークにて接続された他のＰＣ＃２に接続されたものであるとすると、「ＮＧ」という判定結果が得られるので、ＰＣ＃１のＬＣＭ１では、それ以降のチェックアウトのための処理を中断する。

【０１１１】あるいは、終了予定時刻Ｔ’が経過しても当該読み書き処理動作が終了していないとき、判定結果を「ＮＧ」としてもよい。

【０１１２】あるいは、タイムアウト判定部４は２つのモードで動作する。１つは、データサイズ入力部１０１にデータサイズｓが入力されたときで、このとき、タイムアウト判定部は終了予定時刻Ｔ’＝Ｔ＋ｓ／ｂを算出して、それを終了予定時刻格納部１１１に格納する。タイムアウト判定部４は、判定終了信号を受け取ると、現在時刻Ｔと終了予定時刻格納部が格納する時刻Ｔ’とを比較する。前者が後者より小さい場合、タイムアウト判定部４は判定結果ＯＫをＳＭＳ２に通知する。それ以外のときは、判定結果ＮＧをＳＭＳ２に通知する。

【０１１３】他方のモードの動作は、判定開始信号入力部１０２に判定開始信号が入力された場合で、タイムアウト判定部４は、現在時刻Ｔ＋タイムアウト時間ｔを終了予定時刻格納部１１１に格納する。タイムアウト判定の動作は上記一方のモードの場合と同様である。

【０１１４】（秘匿領域）本発明のＬＣＭ１では、チェックイン／チェックアウトのための宿帳を格納する為に、秘匿領域を利用する。ＬＣＭ１をＰＣで構成する場合、この秘匿領域はハードディスク（ＨＤＤ）上に作成される。

【０１１５】ここでは、ＨＤＤ上の秘匿領域について説明する。

【０１１６】ＨＤＤ上には通常パーティションが存在する。パーティションは、ＯＳから１つのドライブとして認識される。各パーティション内に複数のセクターが存在し、データはセクター上に記録される。セクター内のデータ配置を論理フォーマットと呼ぶ。ファイルシステムは、通常ファイル配置テーブルを有する。ファイル配置テーブルには、各ファイル及びディレクトリのセクター上の位置が記録されている。ＯＳは、ファイル配置テーブルを参照して、アクセス対象ファイルの位置を取得し、対象ファイルに到達する。セクターの物理的配置を物理フォーマットと呼ぶ。各パーティションは異なった物理フォーマットを有する事ができる。セクターの位置はヘッドの位置によって識別される。各セクターの開始位置は、磁気的なマークによって識別される。

【０１１７】ＯＳがサポートするファイルシステムについて、ＯＳはドライバを持っている。ドライバは当該ファイルシステムの物理フォーマット及び論理フォーマッ

トを認識しており、パーティション内のセクターを辿ってファイル配置テーブルや各ファイルに到達し、その内容を読み書きする事ができる。

【０１１８】本発明の秘匿領域を構成するためのファイルシステムを図２４に示す。通常のファイルシステムでは、セクターは等間隔に配置されるが、本ファイルシステムでは、そうなっていない。第１セクターの先頭には、セクター配置テーブルがある。セクター配置テーブルは次の形でセクター位置が記録されている。

【０１１９】

ヘッド位置＃２、ヘッド位置＃３、…、ヘッド位置＃ｎ順に、第２セクター、第３セクター、…、第ｎセクターの位置を示している。セクター配置テーブルは暗号化されている。この暗号化を解く鍵は、システムの固有ＩＤに依存する。システム固有のＩＤとしては、例えばＯＳのＩＤ、ＢＩＯＳのＩＤ或いはＣＰＵのＩＤなどが用いられる。

【０１２０】更に、第２セクターの先頭には、ファイル配置テーブルが存在する。これは次の形式である。

【０１２１】

（ファイル１、（セクター番号、セクター内位置））、（ファイル２、（セクター番号、セクター内位置））、…

セクター内位置は、セクター先頭からのバイト数である。ファイル配置テーブルも又暗号化されている。この暗号鍵も又、システム固有のＩＤに依存している。

【０１２２】本発明のファイルシステムに対するアクセスは、特別なドライバ（図１の秘匿領域ドライバ７）を用いて行う。秘匿領域ドライバ７の動作を図２５に示す。当該ドライバ７は又、セクター配置を変更する機能を有している。セクター配置更新時の秘匿領域ドライバ７の動作を図２６に示す。

【０１２３】（認証）以上の説明において、例えば、ＬＣＭ１にＭＣ１３をセットした際に行われる相互認証や、秘匿領域にアクセスする際に行われる認証処理の一例を挙げる。これは、従来からあるもので、公開鍵暗号方式を用いた認証であるが、本発明はこれに限定するものではない。

【０１２４】図２０において、２つの機器（例えば、ＬＣＭ１とＭＣ１３）間でＡからＡにアクセスしようとしているＢを認証する場合について説明する。

【０１２５】この場合、機器Ａは、公開鍵ｋｐを保持しており、機器Ａにアクセス可能であるならば、機器Ｂは、公開鍵ｋｐに対応する秘密鍵ｋｓを保持している。機器Ｂは、機器Ａで発生された乱数Ｒを受け取ると、それを秘密鍵ｋｓで暗号化して（ｋｓ［Ｒ］と表す）、ｋｓ［Ｒ］を機器Ａに返す。機器Ａでは、公開鍵を用いて、ｋｓ［Ｒ］を復号し、復号結果が先に発生した乱数Ｒに等しければ、機器Ｂは正しい相手であると判定する。

【０１２６】その後、上記と同じことを機器Ｂから機器Ａに対して行うことで、相互認証を行うことができる。この場合、機器Ｂは公開鍵を保持し、機器Ａは秘密鍵を保持し、機器Ａが機器Ｂにて発生した乱数を秘密鍵で暗号化してそれを機器Ｂで公開鍵を用いて復号し、先に発生した乱数に等しいかを確認する。

【０１２７】

【発明の効果】以上説明したように、本発明によれば、複製コンテンツの数を効率よく規制して、コンテンツの著作権保護を可能にする。

【図面の簡単な説明】

【図１】本発明の実施形態に係る記憶媒体（メディア）に記憶できる複製コンテンツの数を規制するためのコンテンツ管理方法を用いた音楽コンテンツ利用管理システム（ＬＣＭ）の構成例を示した図。

【図２】メモリ領域の構成例を示した図。

【図３】記録再生装置（ＰＤ）の内部構成例を示した図。

【図４】３種類の記憶媒体の特徴を説明するための図。

【図５】メディアインタフェース（Ｉ／Ｆ）部の内部構成例を示した図。

【図６】チェックイン後の記憶媒体の記録内容を説明するための図。

【図７】ＬＣＭの秘匿領域に格納されている宿帳の記憶例を示した図。

【図８】ＬＣＭの秘匿領域に格納されている宿帳の他の記憶例を示した図。

【図９】チェックイン／チェックアウト処理手順を説明するためのフローチャートで、メディアの種別を判別して、その種別に応じた処理を選択するまでの手順を示したものである。

【図１０】記憶媒体の種別がレベル２の場合のチェックアウト手順を説明するための図。

【図１１】記憶媒体の種別がレベル２の場合のチェックイン手順を説明するための図。

【図１２】記憶媒体の種別がレベル２の場合の再生手順を説明するための図。

【図１３】記憶媒体の種別がレベル１の場合のチェックアウト手順を説明するための図。

【図１４】記憶媒体の種別がレベル１の場合の再生手順を説明するための図。

【図１５】記憶媒体の種別がレベル０の場合のチェックアウト手順を説明するための図。

【図１６】記憶媒体の種別がレベル０の場合のチェックイン手順を説明するための図。

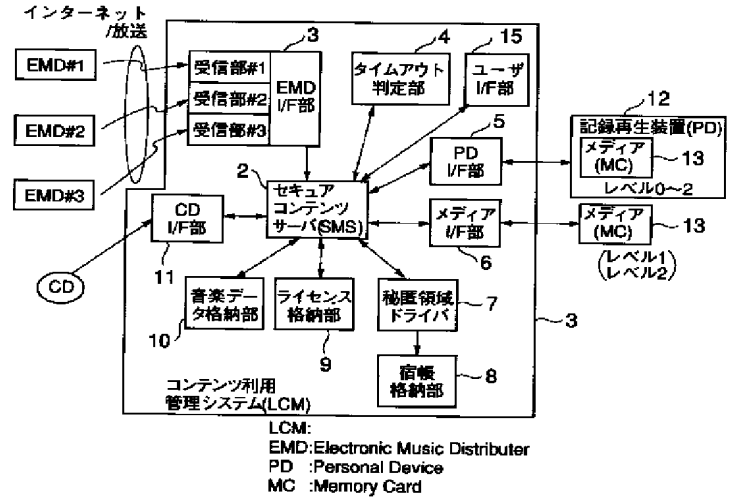
【図１７】記憶媒体の種別がレベル０の場合の再生手順を説明するための図。

【図１８】ＬＣＭの秘匿領域に格納されている宿帳のさらに他の記憶例を示した図で、フラグを含む宿帳を示したものである。

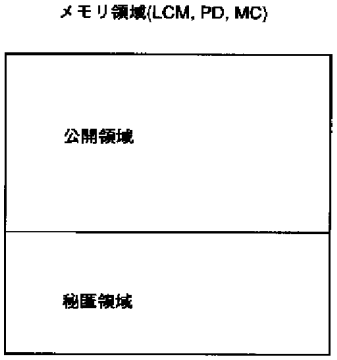
【図１９】フラグを用いたチェックイン処理の概略を説明するためのフローチャート。
【図２０】公開鍵暗号化方式を用いた認証手順を説明するための図。
【図２１】ネットワークを介して記憶媒体への複製コンテンツの記録を行う場合の機器構成例を示した図。
【図２２】タイムアウト判定部の内部構成例を示した図。
【図２３】タイムアウト判定処理の一例を説明するためのフローチャート。
【図２４】秘匿領域を構成するためのファイルシステムを説明するための図。
【図２５】秘匿領域ドライバの動作を説明するためのフローチャート。
【図２６】セクター配置更新時の秘匿領域ドライバの動作を説明するためのフローチャート。

【符号の説明】
１…コンテンツ利用管理システム
２…セキュアコンテンツサーバ（ＳＭＳ）
３…ＥＭＤインタフェース部
４…タイムアウト判定部
５…ＰＤインタフェース（Ｉ／Ｆ）部
６…メディアインタフェース（Ｉ／Ｆ）部
７…秘匿領域ドライバ
８…宿帳格納部
９…ライセンス格納部
１０…音楽データ格納部
１１…ＣＤインタフェース（Ｉ／Ｆ）部
１２…記録再生装置（ＰＤ）
１３…記憶媒体（ＭＣ）

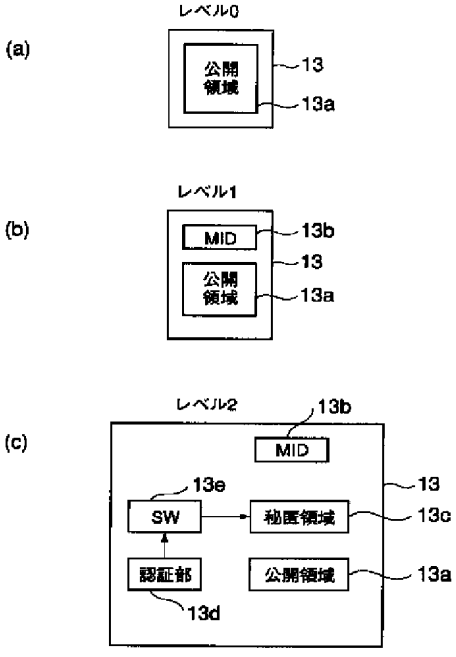
【図１】



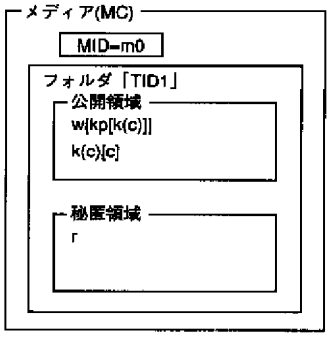
【図２】



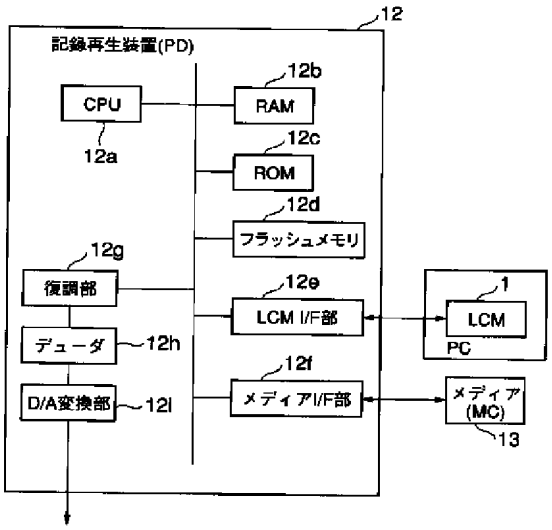
【図４】



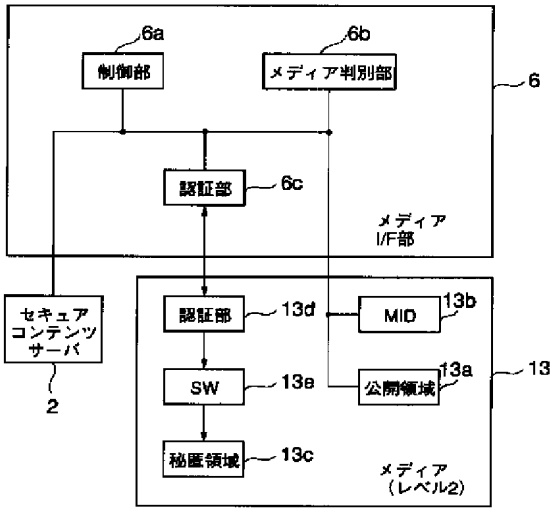
【図６】



【図３】

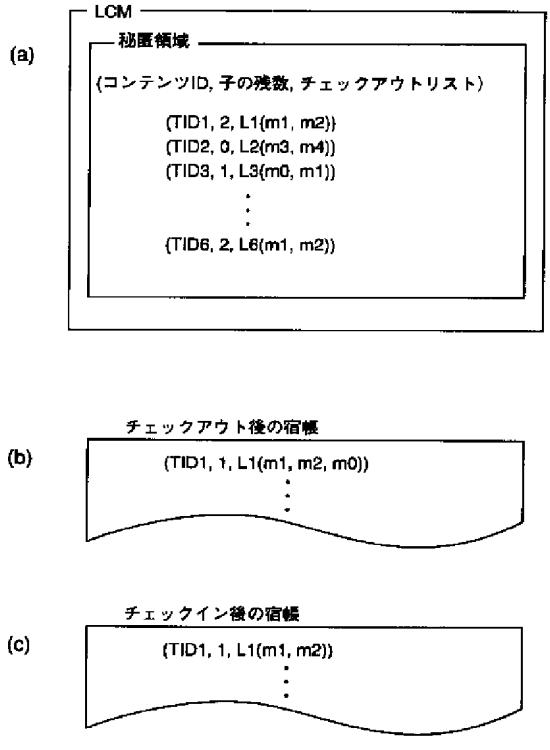


【図５】

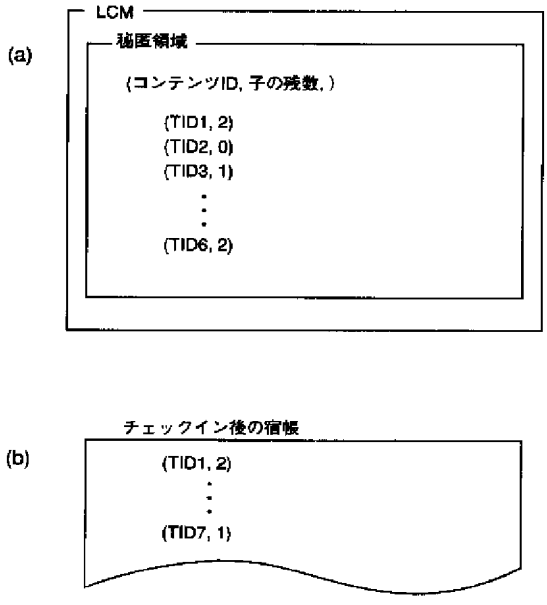


レベル1
MIDのみ

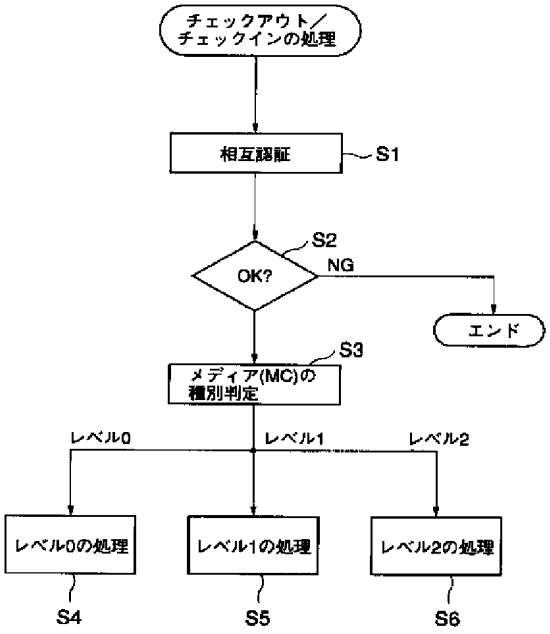
【図７】



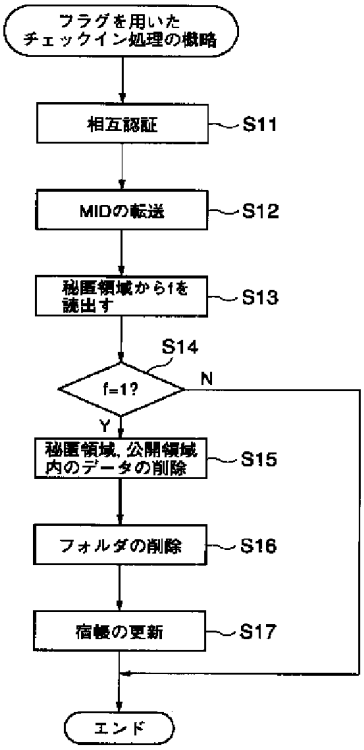
【図８】



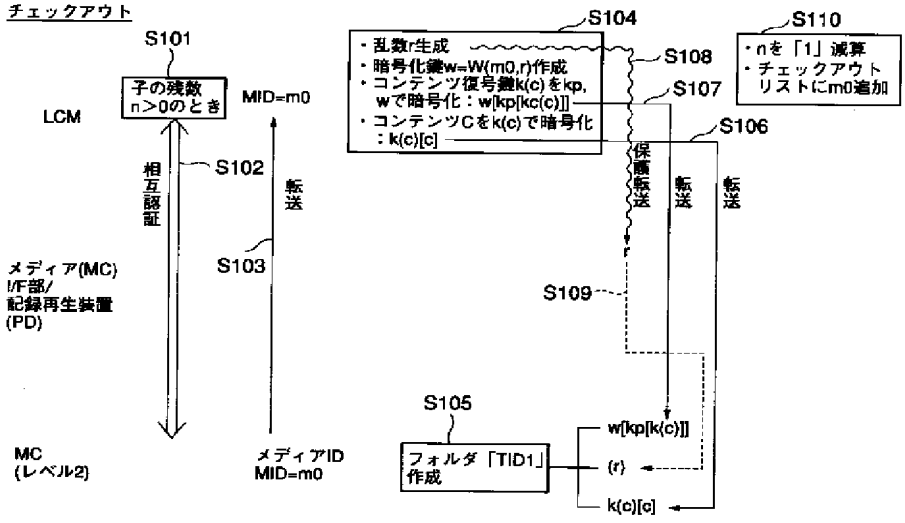
【図９】


チェックアウト／
チェックインの処理
相互認証
S1
S2
OK?
NG
エンド
S3
メディア(MC)の
種別判定
レベル0
レベル1
レベル2
レベル0の処理
レベル1の処理
レベル2の処理
S4
S5
S6

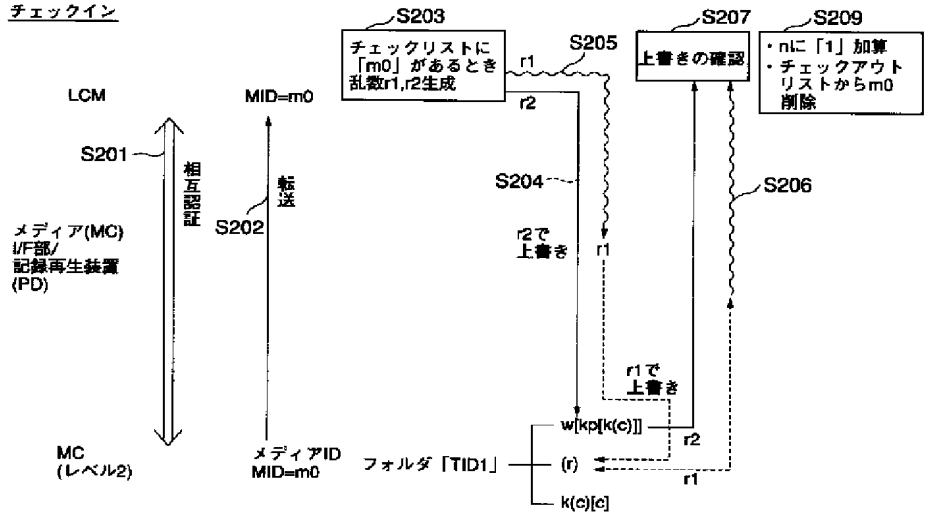
【図１９】


フラグを用いた
チェックイン処理の概略
相互認証
S11
MIDの転送
S12
秘匿領域からfを
読出す
S13
S14
f=1?
N
Y
秘匿領域，公開領域
内のデータの削除
S15
フォルダの削除
S16
宿帳の更新
S17
エンド

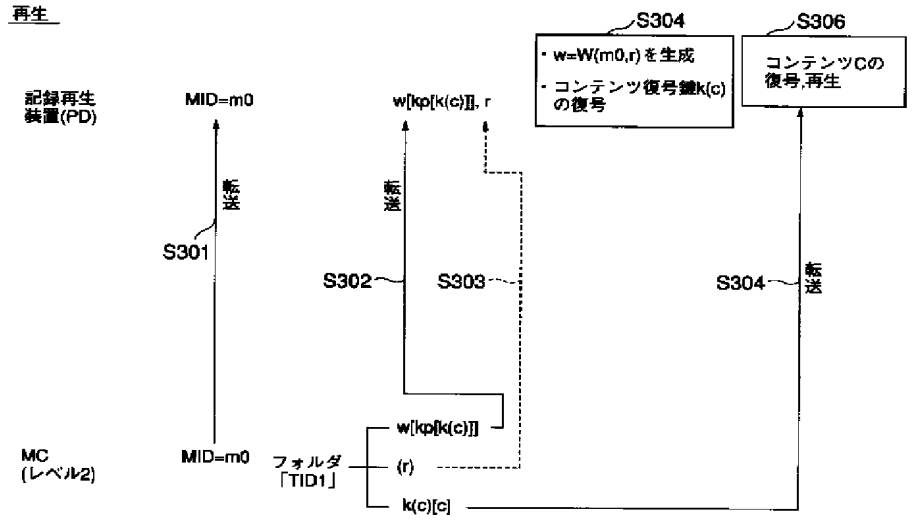
【図１０】


チェックアウト
S101
子の残数
n>0のとき
LCM
MID=m0
相互認証
S102
転送
S103
メディア(MC)
I/F部/
記録再生装置
(PD)
MC
(レベル2)
メディアID
MID=m0
S104
・乱数r生成
・暗号化鍵w=W(m0,r)作成
・コンテンツ復号鍵k(c)をkp,
wで暗号化：w[kp[kc(c)]]
・コンテンツCをk(c)で暗号化
：k(c)[c]
S108
S107
S106
保護転送
転送
転送
r
S109
S110
・nを「1」減算
・チェックアウト
リストにm0追加
S105
フォルダ「TID1」
作成
w[kp[k(c)]]
{r}
k(c)[c]

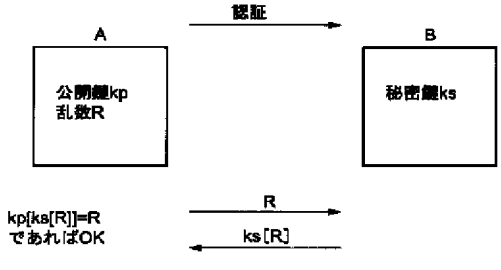
【図１１】



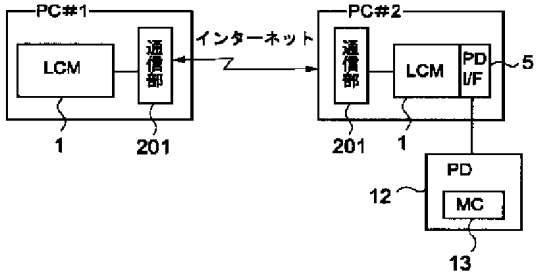
【図１２】



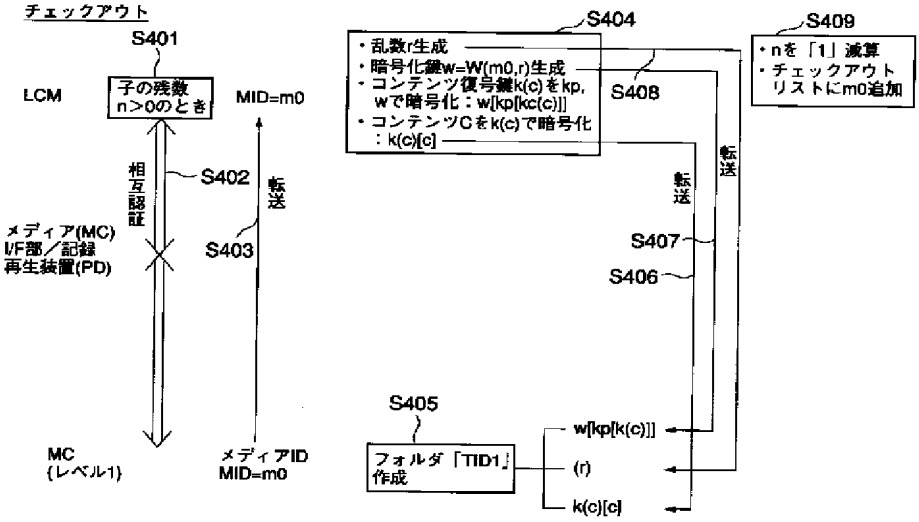
【図２０】



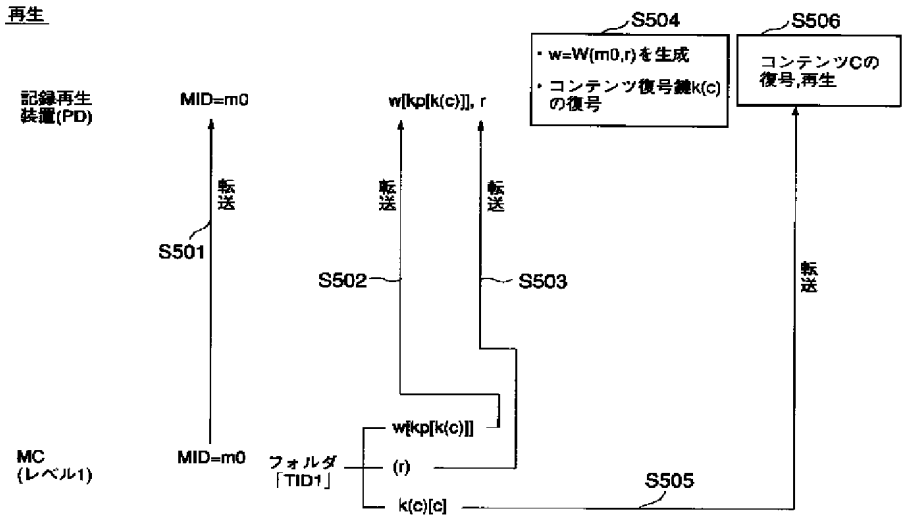
【図２１】



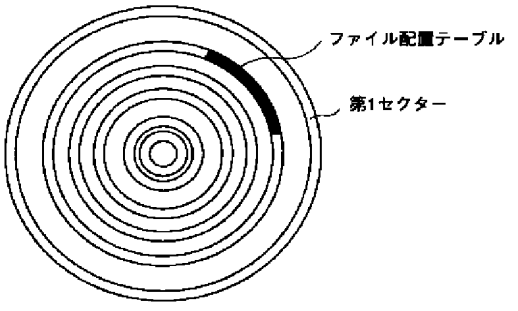
【図１３】



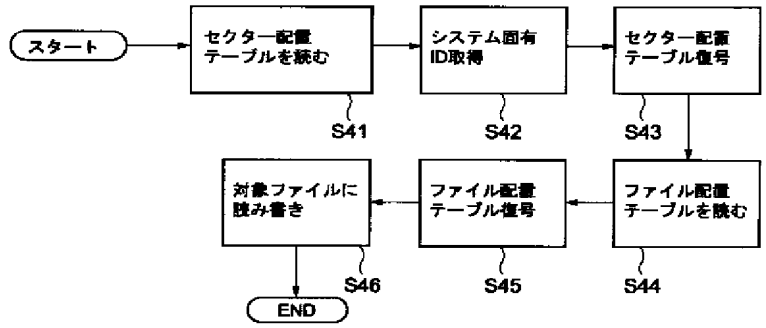
【図１４】



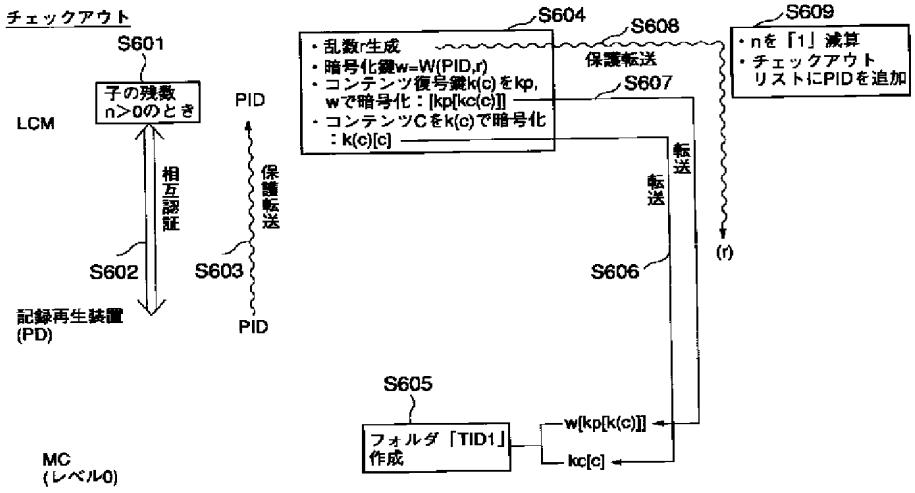
【図２４】



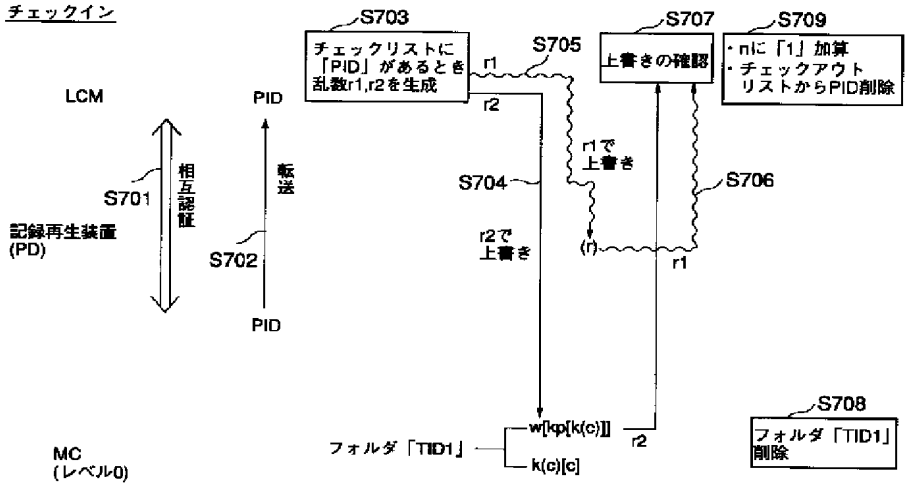
【図２５】



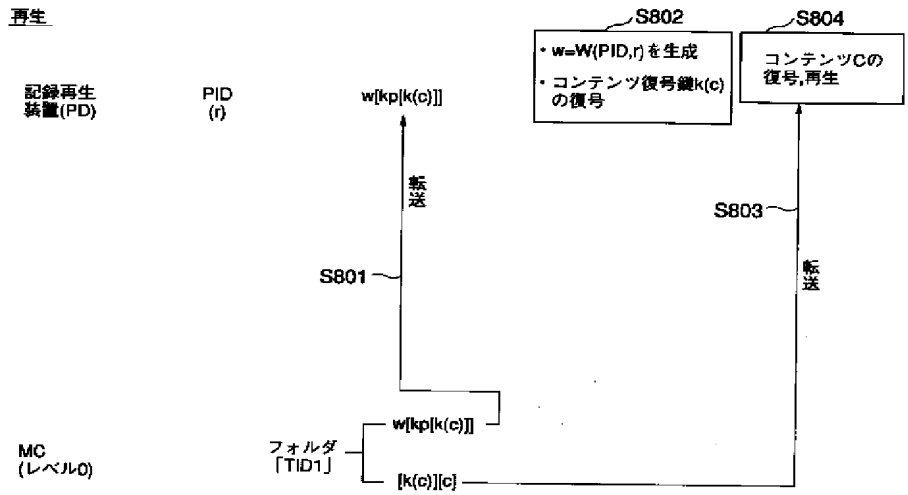
【図１５】


チェックアウト
S601
子の残数
n>0のとき
LCM
相互認証
S602
記録再生装置
(PD)
PID
保護転送
S603
PID
S604
・乱数r生成
・暗号化鍵w=W(PID,r)
・コンテンツ復号鍵k(c)をkp,
wで暗号化：[kp[kc(c)]]
・コンテンツCをk(c)で暗号化
：k(c)[c]
S608
保護転送
S609
・nを「1」減算
・チェックアウト
リストにPIDを追加
S607
転送
転送
S606
(r)
S605
フォルダ「TID1」
作成
w[kp[k(c)]]
kc[c]
MC
(レベル0)

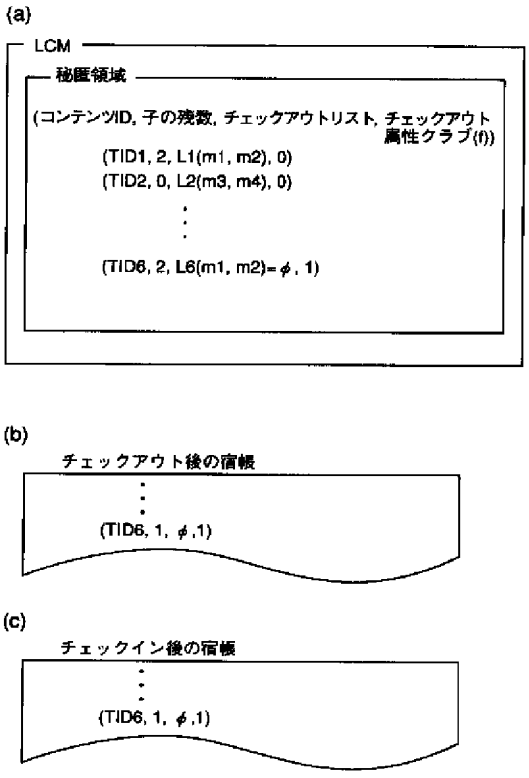
【図１６】


チェックイン
LCM
S701
相互認証
記録再生装置
(PD)
PID
転送
S702
PID
S703
チェックリストに
「PID」があるとき
乱数r1,r2を生成
r1
S705
r2
S704
r1で
上書き
r2で
上書き
(r)
S707
上書きの確認
S706
r1
S709
・nに「1」加算
・チェックアウト
リストからPID削除
S708
フォルダ「TID1」
削除
フォルダ「TID1」
w[kp[k(c)]]
k(c)[c]
r2
MC
(レベル0)

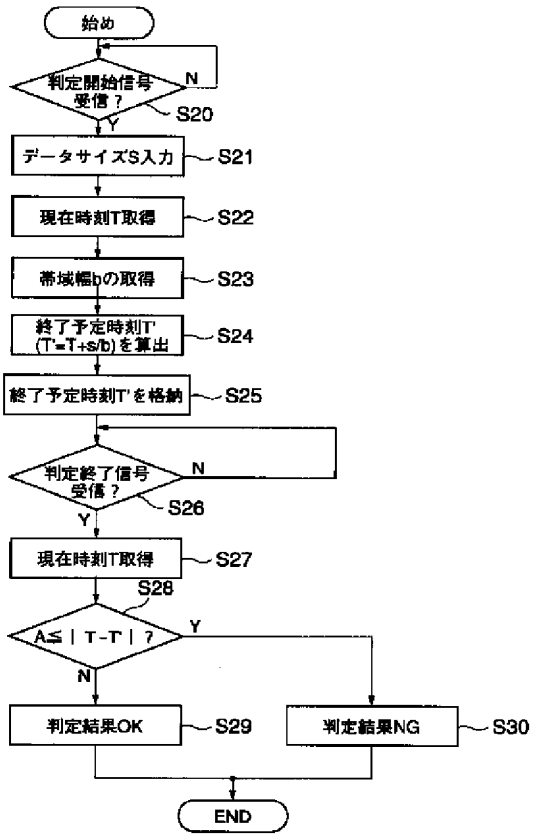
【図17】


再生
記録再生装置(PD)
PID (r)
w[kp[k(c)]]
S802
・w=W(PID,r)を生成
・コンテンツ復号鍵k(c)の復号
S804
コンテンツCの復号,再生
転送
S801
S803
転送
w[kp[k(c)]]
MC (レベル0)
フォルダ「TID1」
[k(c)][c]

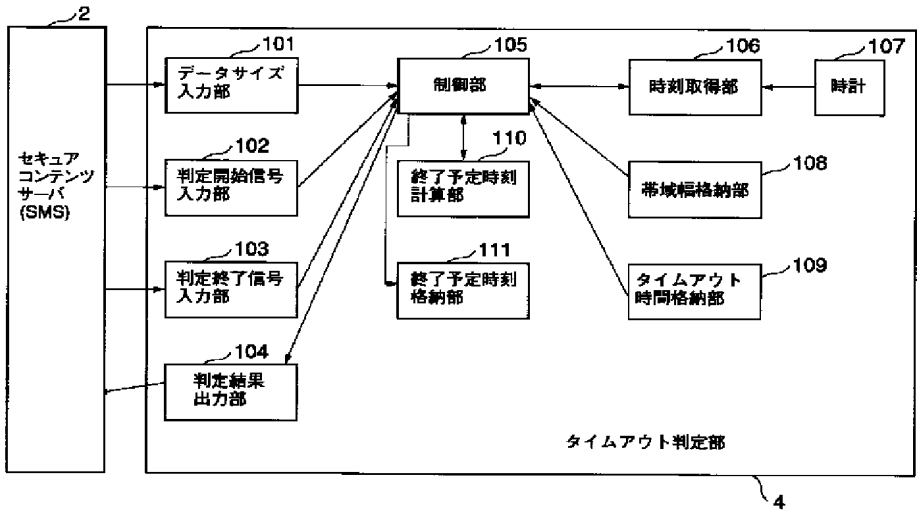
【図18】


(a)
LCM
秘匿領域
(コンテンツID, 子の残数, チェックアウトリスト, チェックアウト属性クラブ(f))
(TID1, 2, L1(m1, m2), 0)
(TID2, 0, L2(m3, m4), 0)
(TID6, 2, L6(m1, m2)=φ, 1)
(b)
チェックアウト後の宿帳
(TID6, 1, φ,1)
(c)
チェックイン後の宿帳
(TID6, 1, φ,1)

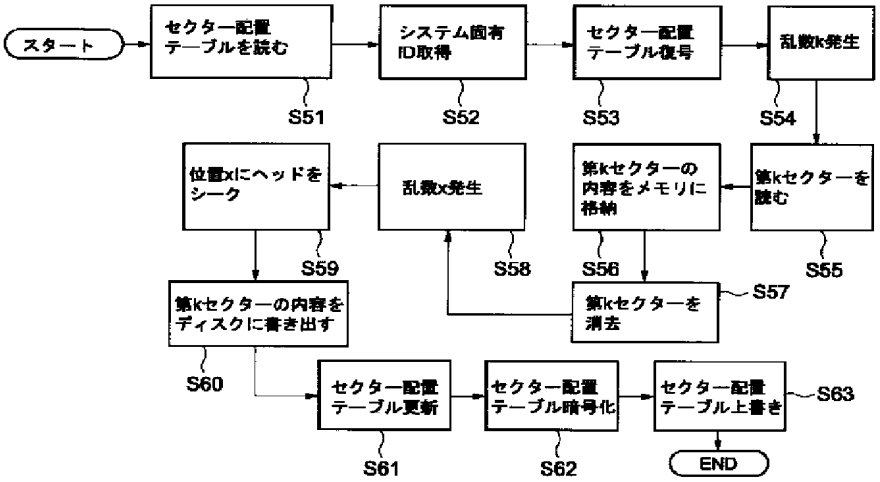
【図23】


始め
判定開始信号受信？
N
Y
S20
データサイズS入力
S21
現在時刻T取得
S22
帯域幅bの取得
S23
終了予定時刻T' (T'=T+s/b)を算出
S24
終了予定時刻T'を格納
S25
判定終了信号受信？
N
Y
S26
現在時刻T取得
S27
S28
A≦｜T-T'｜？
Y
N
判定結果OK
S29
判定結果NG
S30
END

【図２２】



【図２６】



フロントページの続き

(72)発明者　山田　尚志
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内
(72)発明者　石橋　泰博
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内
(72)発明者　加藤　拓
東京都府中市東芝町１番地　株式会社東芝府中工場内
(72)発明者　東間　秀之
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

Ｆターム(参考)　5B017 AA06 BA04 BA05 BA07 BA08
BB10 CA07 CA08 CA09 CA13
CA15 CA16
5B075 KK54 KK68 ND16
5C053 FA13 FA21 FA23 FA27 GB06
GB11 HA29 JA01 JA21 KA04
KA21 KA24 KA25 LA11 LA14